Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Proposed Model for Data Security of Cloud Storage Using Trusted Platform Module

Abhishek Patel* *ABV-IIITM, India.*
Mayank Kumar *ABV-IIITM, India.*

Abstract— Cloud Computing is one of the emerging technologies in Computer Science. Cloud provides various types of services to us. Storage as a Service is generally seen as a good alternative for a small or mid-sized business that lacks the capital budget and/or technical personnel to implement and maintain their own storage. But the main issue is to maintain CIA (Confidentiality, Integrity and Authentication) to the data stored in the cloud. So we have proposed a Trusted Cloud Storage Architecture which applies the specification of Trusted Computing Group (TCG). TCG is a global industry standard, supportive of a hardware-based root of trust, for interoperable trusted computing platforms. We use TPM to encrypt data before storing it to the cloud. And we use Kerberos Authentication Service to avoid masquerading, replay attack and eavesdropping.

Keywords— Cloud, Trusted Computing Group, Trusted Platform Module, Kerberos, Cloud Storage

I. INTRODUCTION

Cloud computing provide a delivery of scalable IT resources over the Internet, as opposed to hosting and operating those resources locally, such as on a college or university network. Resources like applications and services, as well as the infrastructure on which they operate. With cloud computing. Cloud providers specialize in particular applications and services, and this expertise allows them to efficiently manage upgrades and maintenance, backups, disaster recovery, and failover functions. Cloud computing encourages IT organizations and providers to increase standardization of protocols and processes so that the many pieces of the cloud computing model can interoperate properly and efficiently. Cloud computing's scalability is another key benefit to higher education, particularly for research projects that require vast amounts of storage or processing capacity for a limited time. Some companies have built Data Centres near sources of renewable energy, such as wind farms and hydroelectric facilities, and cloud computing affords access to these providers of "green IT". Finally, cloud computing allows college and university IT providers to make IT costs transparent and thus match consumption of IT services to those who pay for such services. There are many services provided by the cloud [4] - (Fig. 1) Application as a Service (AaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). In Software as a Service model, a pre-made application, along with any required software, operating system, hardware, and network are provided. In PaaS, an operating system, hardware, and network are provided, and the customer installs or develops its own software and applications. The IaaS model provides just the hardware and network; the customer installs or develops its own operating systems, software and applications. Storage as a Service (SaaS) [6] is a business model in which a large company rents space in their storage infrastructure to a smaller company or individual.

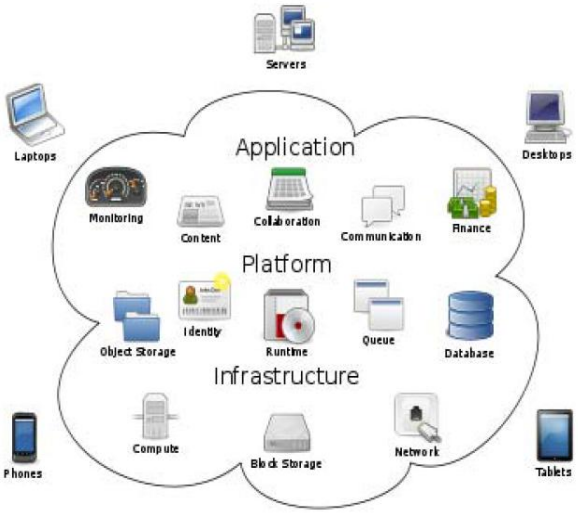

Fig. 1 Various services provided by the cloud

In the enterprise, SaaS vendors are targeting secondary storage applications by promoting SaaS as a convenient way to manage backups. The key advantage to SaaS in an enterprise is in cost savings in personnel, hardware and physical storage space. For instance, instead of maintaining a large tape library and arranging to vault (store) tapes offsite, a network administrator that used SaaS for backups could specify what data on the network should be backed up and how often it should be backed up. The SaaS provider agreed to rent storage space on a cost-per-gigabyte-stored and cost-per-data-transfer basis and the company's data would be automatically transferred at the specified time over the storage provider's proprietary wide area network (WAN) or the Internet. If the company's data ever became corrupt or got lost, the network administrator could contact the SaaS provider and request a copy of the data.

II. DATA STORAGE IN CLOUD AND SECURITY

Storage as a Service is generally seen as a good alternative for a small or mid-sized business that lacks the capital budget and/or technical personnel to implement and maintain their own storage infrastructure. SaaS is also being promoted as a way for all businesses to mitigate risks in disaster recovery, provide long-term retention for records and enhance both business continuity and availability. It seems that every software vendor has become a SaaS vendor, and every hardware vendor has begun supporting the cloud. New applications are being offered in the cloud, and businesses are beginning to use cloud infrastructure to run their own custom applications. Companies still think long and hard about moving applications and data to the cloud from traditional, on-premise computing models, and many are hesitating to move applications containing sensitive data. The benefits of cloud computing are significant—economies of scale, potential cost savings, fast deployment and easy scalability. For many businesses, essential questions about security, privacy, compliance, and control of corporate data remain unanswered. According to the research report, *KPMG's 2010 Cloud Computing Survey, 2010*, security is the biggest obstacle to cloud adoption (as shown in the fig.2), followed closely by legal, compliance, and privacy issues.

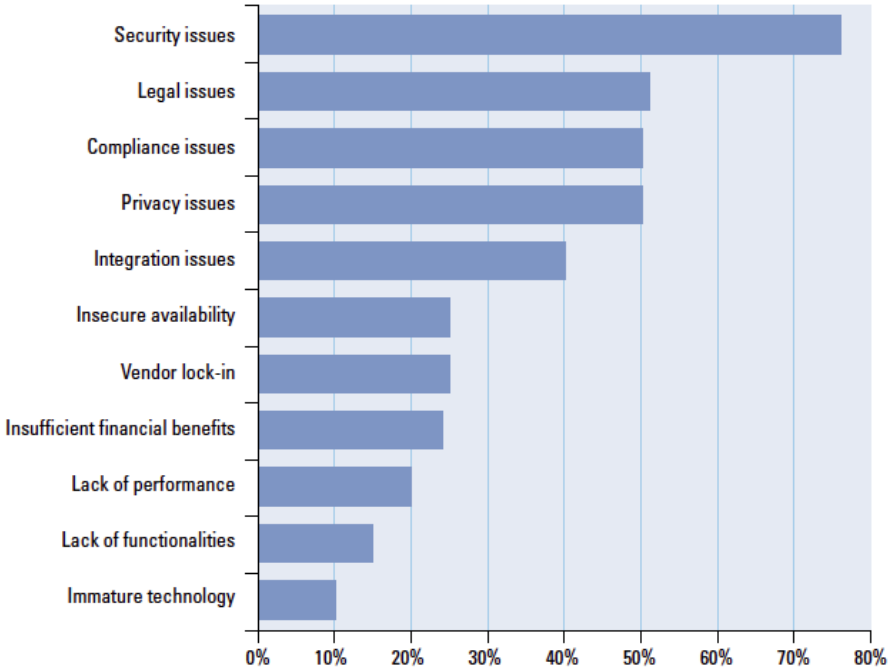

Fig. 2 Main concern regarding the use of cloud computing

According to the *Goldman Sachs Equity Research Report of 2011*, 70% of the CIOs surveyed express major concerns about data security in the cloud. Their concerns include the loss of transparency and control over where business data resides and how it is protected outside the enterprise, in the cloud provider infrastructure. Cloud computing has brought advantages in the form of online storage. In this section, we are referring to Storage-as-a-Service. Data security for such a cloud service encompasses several aspects including secure channels, access controls, and encryption. And, when we consider the security of data in a cloud, we must consider the security triad: confidentiality, integrity, and Authentication. One of the more recent trends in online cloud-based storage is the cloud storage gateway. Several vendors offer such solutions that are generally implemented as an appliance that resides onsite at the customer premises.

III. TRUSTED COMPUTING

Encryption is one of the major reasons why online backup is the preferred choice for computer storage. Encryption prevents malicious parties from attempting to access, change or damage files by storing them in a why which is inaccessible without the key. *Trusted Computing* based on hardware root of trust has been developed by industry to protect computing infrastructure and billions of end points. Encryption prevents unwanted individuals from being able to access, tamper with or vindictively change files to cause harm to you personally or to your business. Encryption is the process whereby you use a program to scramble data in a way which can only be rectified by using a key. This protects

the files while they are on our data servers, by simply storing them away from your PC. TCG [1] created the Trusted Platform Module cryptographic capability, which enforces specific behaviours and protects the system against unauthorized changes and attacks such as malware and root kits. As computing has expanded to different devices and infrastructure has evolved, so too has TCG extended the concept of trusted systems well beyond the computer-with-a-TPM to other devices, ranging from hard disk drives and mobile phones. Standards-based Trusted Computing technologies developed by TCG members now are deployed in enterprise systems, storage systems, networks, embedded systems, and mobile devices and can secure cloud computing and virtualized systems.

IV. CLOUD SECURITY

Public and private cloud services, also known as multi-tenant infrastructure, are used increasingly in the enterprise and by government agencies. With their popularity come security issues that are now high priority. A number of TCG technologies and standards, including the Trusted Platform Module (TPM), network security, and self-encrypting drives can be used to provide security for systems, networks, and data. TCG also is addressing how to interface various technical standards to create an end-to-end enterprise solution that is tailored to meet mission and business needs and comply with security policies within public and private cloud networks. TPM (Trusted Platform Module) is a computer chip (microcontroller) that can securely store artifacts used to authenticate the platform (your PC or laptop). These artifacts can include passwords, certificates, or encryption keys. A TPM can also be used to store platform measurements that help ensure that the platform remains trustworthy. Authentication (ensuring that the platform can prove that it is what it claims to be) and attestation (a process helping to prove that a platform is trustworthy and has not been breached) are necessary steps to ensure safer computing in all environments. TPM maintains thrice of all (CIA) properties:

Confidentiality: The nature of hardware-based cryptography ensures that the information stored in hardware is better protected from external software attacks. A variety of applications storing secrets on a TPM can be developed. These applications make it much harder to access information on computing devices without proper authorization.

Authentication: The TPM, a simple, yet revolutionary concept, ensures only authorized users and authorized PCs are on an enterprise network. It also acts as a secure vault for certificates, keys and passwords, negating the need for costly tokens.

Platform Integrity: Measures and reports on the integrity of platform, including the BIOS, disk MBR, boot sector, operating system and application software, to ensure no unauthorized changes have occurred. The TPM, a secure cryptographic integrated circuit (IC), provides a hardware-based approach to manage user authentication, network access, data protection and more that takes security to higher level than software-based security.

V. TRUSTED CLOUD STORAGE ARCHITECTURE

For the vast majority of cloud storage, the security and privacy options provided are perfectly acceptable. The fact is that most people just don't care about privacy. For those of us that do, however, there is a relatively easy solution that can allow you to continue using cloud storage and keep your data secure, Using Trusted Cloud; you can create encrypted folders within your cloud storage, which gets synched like any other file from the Trusted Cloud. You probably have data stored in multiple clouds - Salesforce, Box.net, Gmail, Amazon, and many others. Trusted Cloud provides you with the ability to create a unified data protection policy across all clouds. As an in-line security gateway that sits between your users and your cloud applications, Trusted Cloud applies encryption on the fly before sensitive data leaves the enterprise. By applying encryption in a cloud security gateway, Cipher Cloud eliminates the inherent security and privacy risks of cloud computing. Your business never loses control of its sensitive data, yet you can achieve the full benefits of cloud computing. Mostly data stored in cloud are not in protected format. There is a big concern of security in cloud storage. The Trusted Gateway provides a way to encrypt sensitive information to the enterprises as it moves to any cloud application and then decrypt it again as data is delivered to end users. This protects the data from being accessed by others. This revolutionary technology maintains the cloud application user experience, with near zero latency, and without making any changes to the cloud application itself. Trusted Gateway takes a revolutionary approach to protecting sensitive data before it leaves an organization's secure enterprise network. As illustrated in the fig. 3 the Trusted Gateway examines all outgoing cloud requests, in real time, to identify sensitive data, encrypt that data using TPM, and then forward the modified request to the cloud application. Similarly, encrypted data returning from the cloud application is converted, again in real time, into clear text prior to being displayed to the end user.

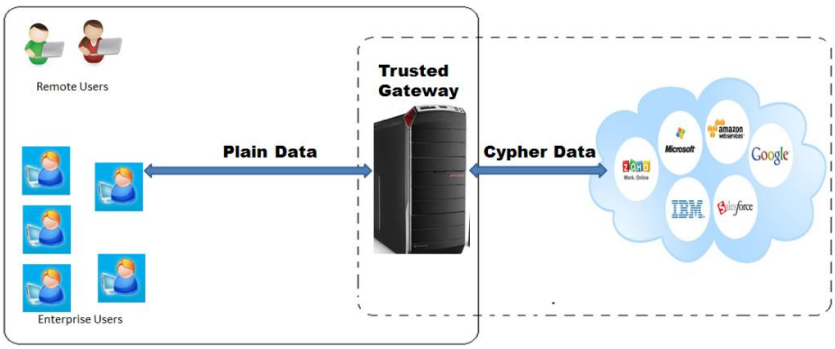

Fig. 3 TrustedCloud Storage Architecture

There also may be possible that in the internal network some intruder gain access pretend to be another genuine user. So it is necessary to authenticate the user to retain security. For authenticate the users we use the famous Kerberos authentication service [2]. The entities of the authentication service are as follows:

End User (U): User, who aims to stores encrypted credentials to the cloud storage. So to encrypt data user should authenticate itself to the Trusted Gateway.

Remote User: Remote User, who access the cloud storage outside the internal enterprise network.

Trusted Gateway (TG): Trusted gateway is the work station having TPM which maintains the data to be encrypted comes from end users and encrypt them and store to the cloud storage and vice versa.

Authentication Server (AS): Authentication Server verifies user's access right in database; create ticket granting ticket and session key.

Ticket Granting Server (TGS): Ticket Granting Server issues ticket to request the Trusted Gateway.

Database: The Kerberos service must have a database to store user id (ID) and hashed passwords.

The details of the Kerberos Authentication Service Exchange are:

A. Authentication Service Exchange to obtain ticket-granting Ticket

(1) **U → AS** : ID_u, ID_{tgc}, TS_1

(2) **AS → U** : $E (K_u , [K_{u,tgs}||ID_{tgs}||TS_2 ||Lifetime_2 ||Ticket_{tgs}])$

$Ticket_{tgs}= E(K_{tgs}, [K_{u,tgs}||ID_u||AD_u||ID_{tgs}||TS_2 ||Lifetime_2])$

B. Ticket-granting service Exchange to obtain trusted gateway service-granting ticket

(3) **U → TGS** : $ID_{tg}||Ticket_{tgs}||Authenticator_u$

(4) **TGS → U** : $E(K_{u,tgs},[K_{u,tg}||ID_{tg}||TS_4 ||Ticket_{tg}])$

$Ticket_{tg}= E(K_{tg},[K_{u,tg}||ID_u||AD_u||ID_{tg}||TS_4 ||Lifetime_4])$

$Authenticator_u= E(K_{u,tgs}||ID_u||AD_u||TS_3)$

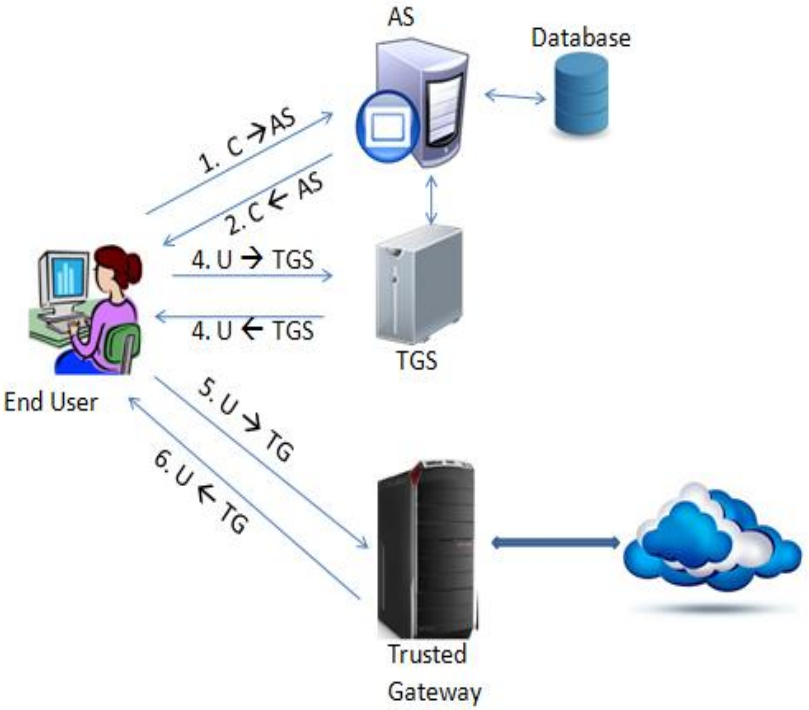

Fig. 4 Kerberos authentication service

C. User /trusted gateway Authentication Exchange to obtain cloud service

(1) **U → TG** : $Ticket_{tg}||Authenticator_u$

(2) **TG → U** : $E(K_{u,tg},[TS_5 +1])$

$Authenticator_u= E(K_{u,tg}||ID_u||AD_u||TS_5)$

Once the session is created between end user and trusted gateway then the end user can send data to store in the cloud in encrypted form and also can retrieve data from the cloud with the help of Trusted Gateway. Records of data sent and retrieved to the cloud from various end users is maintains by the Trusted Gateway. As we clarify that the data which is stored in the cloud in the encrypted form in highly confidential so to keep the security of data we assume that the remote users who want to retrieve the data from cloud have TPM chip in his system. So remote users have to authenticate itself to the trusted gateway and then it can exchange keys, by which it can retrieve data directly from the cloud and decrypt itself.

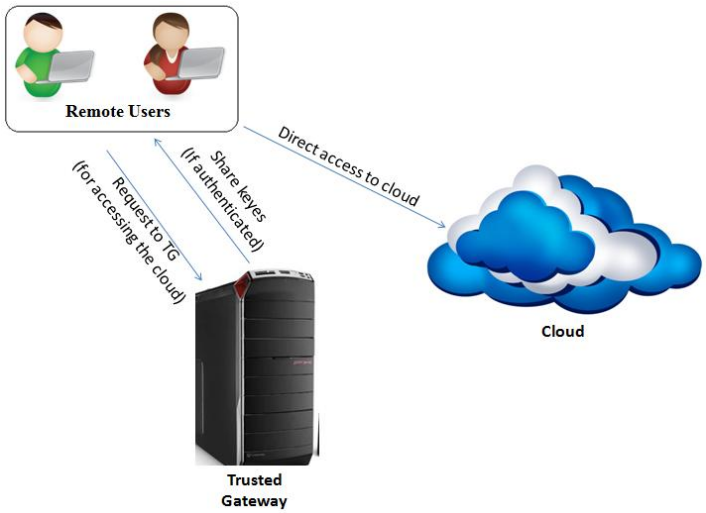

Fig. 5 Creating remote session to the cloud

VI. CONCLUSIONS

In this paper we have proposed a model which helps to use trusted platform module widely for the security of cloud storage. We have design a new trust model which uses TPM store encrypted data to the cloud, which is unprofitable to the other users. The data will be safe in the public cloud also. Kerberos is the secure method to authenticating requests for any service, is used to authenticate end users to the trusted gateway. In TPM access to keys, data or systems is often protected and requires authentication by presenting a password.

REFERENCES

[1] Trusted Computing Group.[Online].Available: https://www.trustedcomputinggroup.org/

[2] William Stallings, *Cryptography and Network Security- Principles and Practices*, 3rd Edition, Prentice Hall of India, 2003.

[3] K.Valli Madhavi, R. Tamilkodi and R.Bala Dinakar, "Data Storage Security in Cloud Computing for Ensuring Effective and Flexible Distributed System," *International Journal of Electronics Communication and Computer Engineering*, Volume 3, Issue (1) NCRTCST, ISSN 2249 –071X.

[4] Shyam Patidar, Dheeraj Rane and Pritesh Jain, "A Survey Paper on Cloud Computing," 2012 Second International Conference on Advanced Computing & Communication Technologies."

[5] Kailash Patidar, Ravindra Gupta, Gajendra Singh, Megha Jain and Priyanka Shrivastava, "Integrating the Trusted Computing Platform into the Security of Cloud Computing System," *International Journal of Advanced Research in Computer Science and Software Engineering*, ISSN: 2277 128X, Volume 2, Issue 2, February 2012.

[6] Gurudatt Kulkarni, Ramesh Sutar and Jayant Gambhir, "Cloud Computing-Storage as Service," *International Journal of Engineering Research and Applications (IJERA)*, ISSN: 2248-9622, Vol. 2, Issue 1, Jan-Feb 2012, pp.945-950.

[7] S.Sajithabanu and E.George Prakash Raj, "Data Storage Security in Cloud," *International Journal of Computer Science and Technology*, ISSN: 0976-8491 (Online)| ISSN: 2229-4333 (Print), IJCST Vol. 2, Issue 4, Oct. -Dec. 2011.

[8] Hari Baaskar R and Gomathi A, "A Framework for Security Based Cloud by using Trusted Computing," *International Journal of Advanced Research in Computer Science and Software Engineering*, ISSN: 2277 128X, Volume 2, Issue 12, December 2012.

[9] Nashaat el-Khameesy and Hossam Abdel Rahman, "A Proposed Model for Enhancing Data Storage Security in Cloud Computing Systems," *Journal of Emerging Trends in Computing and Information Sciences*, ISSN 2079-8407, Vol. 3, Nn. 6, June 2012.

[10] Cong Wang, Qian Wang, KuiRen, Ning Cao and Wenjing Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," *Services Computing, IEEE Transactions on* , vol.5, no.2, pp.220,232, April-June 2012.

[11] Mehdi Hojabr, "Ensuring data storage security in cloud computing with effect of kerberos," *International Journal of Engineering Research & Technology (IJERT)*,ISSN-2278-0181, Vol. 1, issue 5, July - 2012.

